CLAIMS

What is claimed is:

1. A method for protecting the identity of one or more hidden recipients of an email message, the email message comprising an email header and an email body, the method comprising:

creating a first encrypted email body by encrypting the email body using a first encryption key;

creating a second encrypted email body by encrypting the email body using a second encryption key;

creating a first encrypted email message comprising the first encrypted email body and, for each of one or more revealed recipients, an encrypted version of the first encryption key;

creating a second encrypted email message comprising the second encrypted email body and, for each of the one or more hidden recipients, an encrypted version of the second encryption key;

transmitting the first encrypted email message to the one or more revealed recipients; and

transmitting the second encrypted email message to the one or more hidden recipients.

2. The method of claim 1 further comprising: determining the one or more revealed recipients of the email message and determining the one or more hidden recipients of the email message.

3. The method of claim 2, wherein the email header comprises a TO field, a CC field, and a BCC field, and wherein further the one or more revealed recipients are determined by reference to the TO field and the CC field and the one or more hidden recipients are determined by reference to the BCC field.

4. The method of claim 1, wherein the first encryption key and the second encryption key are equivalent, and wherein the first encrypted email body and the second encrypted email body are equivalent.

5. The method of claim 1, wherein the creating the first encrypted email message comprises:

locating one or more revealed recipient certificates corresponding to the one or more revealed recipients;

obtaining one or more revealed recipient public keys corresponding to the one or more revealed recipients from the one or more revealed recipient certificates; and

encrypting, for each of one or more revealed recipients, the first encryption key using the one or more revealed recipient public keys;

and wherein the creating the second encrypted email message comprises:

locating one or more hidden recipient certificates corresponding to the one or more hidden recipients;

obtaining one or more hidden recipient public keys corresponding to the one or more hidden recipients from the one or more hidden recipient certificates; and encrypting, for each of one or more hidden recipients, the second encryption key using the one or more hidden recipient public keys.

6. The method of claim 1, wherein the creating the second encrypted email message comprises creating one or more encrypted email messages corresponding to the one or more hidden recipients, wherein each encrypted email message of the one or more encrypted email messages comprises the second encrypted email body and the second encryption key encrypted for a corresponding hidden recipient; and wherein the transmitting the second encrypted email message comprises transmitting the one or more encrypted email messages to the corresponding one or more hidden recipients.

7. The method of claim 6, wherein the one or more hidden recipients are members of an email mailing list referenced in the email header.

8. A computer-readable medium having computer-executable instructions for protecting the identity of one or more hidden recipients of an email message, the email message comprising an email header and an email body, the computer-readable instructions performing steps comprising:

creating a first encrypted email body by encrypting the email body using a first encryption key;

creating a second encrypted email body by encrypting the email body using a second encryption key;

creating a first encrypted email message comprising the first encrypted email body and, for each of one or more revealed recipients, an encrypted version of the first encryption key;

creating a second encrypted email message comprising the second encrypted email body and, for each of the one or more hidden recipients, an encrypted version of the second encryption key;

transmitting the first encrypted email message to the one or more revealed recipients; and

transmitting the second encrypted email message to the one or more hidden recipients.

9. The computer-readable medium of claim 8 having further computer-executable instructions for performing steps comprising: determining the one or more revealed recipients of the email message and determining the one or more hidden recipients of the email message.

10. The computer-readable medium of claim 9, wherein the email header comprises a TO field, a CC field, and a BCC field, and wherein further the one or more revealed recipients are determined by reference to the TO field and the CC field and the one or more hidden recipients are determined by reference to the BCC field.

11. The computer-readable medium of claim 8, wherein the first encryption key and the second encryption key are equivalent, and wherein the first encrypted email body and the second encrypted email body are equivalent.

12. The computer-readable medium of claim 8, wherein the creating the first encrypted email message comprises:

locating one or more revealed recipient certificates corresponding to the one or more revealed recipients;

obtaining one or more revealed recipient public keys corresponding to the one or more revealed recipients from the one or more revealed recipient certificates; and

encrypting, for each of one or more revealed recipients, the first encryption key using the one or more revealed recipient public keys;

and wherein the creating the second encrypted email message comprises:

locating one or more hidden recipient certificates corresponding to the one or more hidden recipients;

obtaining one or more hidden recipient public keys corresponding to the one or more hidden recipients from the one or more hidden recipient certificates; and

encrypting, for each of one or more hidden recipients, the second encryption key using the one or more hidden recipient public keys.

13. The computer-readable medium of claim 8, wherein the creating the second encrypted email message comprises creating one or more encrypted email messages corresponding to the one or more hidden recipients, wherein each encrypted email message

of the one or more encrypted email messages comprises the second encrypted email body and the second encryption key encrypted for a corresponding hidden recipient; and wherein the transmitting the second encrypted email message comprises transmitting the one or more encrypted email messages to the corresponding one or more hidden recipients.

14. The computer-readable medium of claim 13, wherein the one or more hidden recipients are members of an email mailing list referenced in the email header.

15. A computer-readable medium having computer-executable instructions for protecting the identity of one or more hidden recipients of an email message, the email message comprising an email header and an email body, the computer-readable instructions performing steps comprising:

determining one or more revealed recipients of the email message;

determining the one or more hidden recipients of the email message; and

selecting a hidden recipients concealment option;

wherein the one or more revealed recipients will receive a first encrypted email message comprising, for each of one or more revealed recipients, an encrypted version of a first encryption key and a first encrypted email body created by encrypting the email body using the first encryption key; and

wherein further each of the one or more hidden recipients will receive, depending on the selected hidden recipients concealment option, either a second encrypted email message comprising, for each of one or more hidden recipients, an encrypted version of a second encryption key and a second encrypted email body created by encrypting the email body using the second encryption key, or a corresponding one or more encrypted email messages corresponding to the one or more hidden recipients, wherein each encrypted email message of the corresponding one or more encrypted email messages comprises the second encryption key encrypted for a corresponding hidden recipient and a second encrypted email body created by encrypting the email body using the second encryption key.

16. The computer-readable medium of claim 15, wherein the email header comprises a TO field, a CC field, and a BCC field, and wherein further the one or more revealed recipients are determined by reference to the TO field and the CC field and the one or more hidden recipients are determined by reference to the BCC field.

17. The computer-readable medium of claim 15, wherein the first encryption key and the second encryption key are equivalent, and wherein the first encrypted email body and the second encrypted email body are equivalent.

18. The computer-readable medium of claim 13 having further computer-executable instructions for performing steps comprising:

encrypting the first encryption key for each of the one or more revealed recipients;

encrypting the second encryption key for each of the one or more hidden recipients; and

transmitting the encrypted first encryption keys, the encrypted second encryption keys, and an indication of the revealed recipients, the hidden recipients and the selected hidden recipients concealment option to a computing device, the computing device creating and transmitting the first encrypted email message and either the second encrypted email message or the corresponding one or more encrypted email messages depending on the selected hidden recipients concealment option.

19. The computer-readable medium of claim 18, wherein the encrypting the first encryption key comprises:

locating one or more revealed recipient certificates corresponding to the one or more revealed recipients;

obtaining one or more revealed recipient public keys corresponding to the one or more revealed recipients from the one or more revealed recipient certificates; and

encrypting, for each of one or more revealed recipients, the first encryption key using the one or more revealed recipient public keys;

and wherein the encrypting the second encryption key comprises:

locating one or more hidden recipient certificates corresponding to the one or more hidden recipients;

obtaining one or more hidden recipient public keys corresponding to the one or more hidden recipients from the one or more hidden recipient certificates; and

encrypting, for each of one or more hidden recipients, the second encryption key using the one or more hidden recipient public keys.

20. A computer-readable medium having computer-executable instructions for implementing a secure mailing list, the secure mailing list having one or more members, the computer-executable instructions performing steps comprising:

receiving an incoming email comprising a header indicating the incoming email was sent to the secure mailing list and an incoming email body;

encrypting the incoming email body using an encryption key;

encrypting the encryption key for each of the one or more members;

creating one or more encrypted email messages corresponding to the one or more members, wherein each encrypted email message of the one or more encrypted email messages comprises the encryption key, encrypted for a corresponding member, and the encrypted incoming email body; and

transmitting the one or more encrypted email messages to the corresponding one or more members.

21. The computer-readable medium of claim 20, wherein the encrypting the encryption key for each of the one or more members is performed using one or more public keys for each of the one or more members, the one or more public keys obtained from one or more certificates corresponding to each of the one or more members.